УДК 519.713

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІТІВ НА ЕЛІПТИЧНІЙ КРИВІЙ НА ВІДПОВІДНІСТЬ МІЖНАРОДНОМУ СТАНДАРТУ ISO/IEC 18031

Т.О. ГРІНЕНКО, К.А. ПОГРЕБНЯК

Представлені результати дослідження властивостей генераторів псевдовипадкових бітів на еліптичній кривій, які відповідають вимогам міжнародного стандарту ISO/IEC 18031. Надано рекомендації щодо застосування цих генераторів в криптографії.

The results of researching the properties of pseudorandom bit generators on an elliptic curve which meet the requirements of the international standard ISO/IEC 18031 are presented. The recommendations on the use of these generators in cryptography are given.

ВСТУП

Розробка методів генерації випадкових та псевдовипадкових послідовностей і методів та засобів оцінки їх властивостей є дуже актуальним, важливим та необхідним напрямком досліджень. Вихідні дані генераторів випадкових та псевдовипадкових бітів використовуються у багатьох криптографічних додатках, наприклад, при генеруванні ключів, загальносистемних параметрів тощо. При цьому, якщо генератор випадкових бітів є неякісним, то він може легко стати самим вразливим елементом криптографічної системи.

Відповідно до вимог криптографічних додатків генератори псевдовипадкових бітів (ГПВБ) повинні задовольняти ряду складних і суперечливих вимог. Так псевдовипадкові послідовності (ПВП), що генеруються ГПВБ, повинні володіти рядом властивостей «випадковості» їхньої появи, мати необхідний період повторення, високу (необхідну) структурну скритність законів формування й ін. [1, 2]. На наш погляд, цим вимогам значною мірою можуть задовольняти ГПВБ, які розроблені з використанням переваг теоретико-числових задач (наприклад, задачі дискретного логарифма в групі точок еліптичних кривих) [1-3]. При забезпеченні вимог випадковості і/або непередбачуваності такого генератора рішення задачі криптоаналіза буде експоненційно складним.

У загальному випадку для побудови ГПВБ використовується однобічна функція. Для побудови таких однобічних функцій використовуються функції, складність яких ґрунтується на складності дискретного логарифму [4] або на складності факторизації великого числа [5].

В 90-і роки був розроблений математичний апарат і створені криптографічні системи, перетворення в яких здійснювалися в групах точок еліптичних кривих [6]. Також у доступній літературі вказувалося про можливість побудови ГПВБ на еліптичних кривих (ЕК), але ніяких практичних пропозицій щодо цього не було. В 2001 році в [1] був запропонований ГПВБ на ЕК та досліджені властивості сформованих ПВП. Там же були запропоновані метод і алгоритми побудови ПВП в групах точок ЕК над простим полем $GF(P)$. Стійкість такого генератора на ЕК засновано на складності вирішення задачі дискретного логарифму, яка полягає у складності знаходження цілого a, такого що $y \equiv g^a \pmod p$ [7].

Має сенс рішення цієї задачі на загальний випадок розширеного поля в різних поданнях ЕК і з різними реалізаціями алгоритмів побудови ПВП. В 2002 році ця задача була вирішена, результати представлені в [2]. Були запропоновані декілька алгоритмів побудови ГПВБ на ЕК та проведені дослідження статистичних характеристик отриманих ПВП, а також порівняльний аналіз цих генераторів із класичним BBS-генератором [8]. Стійкість генератора на ЕК, що був запропонований в [2], засновано на задачі дискретного логарифму в групі точок еліптичної кривої. Сутність її в тому, що для заданих точок P і Q на еліптичній кривій порядку n необхідно знайти таке число a, щоб $Q = aP$.

В 2005 році був прийнятий міжнародний стандарт ISO/IEC 18031 «Інформаційні технології – Методи захисту – Генерація випадкових бітів», який містить вимоги щодо генерування випадкових та псевдовипадкових бітів. В цьому стандарті для використання в криптографічних додатках було запропоновано три типи ГПВБ: на базі використання геш-функції, блокового шифру та перетворень на ЕК.

Метою цієї статті є аналіз та порівняння властивостей ПВП, що отримані за допомогою ГПВБ на ЕК, які представлені в ISO/IEC 18031 та в [2]. У відповідності з ISO/IEC 18031 та [1, 2] були реалізовані програмні моделі ГПВБ на еліптичній кривій та досліджені їх властивості.

1. ОПИС ГПВБ НА ЕК СТАНДАРТУ ISO/IEC 18031

Як уже вказувалось, в стандарті ISO/IEC 18031, в залежності від вимог зі сторони криптографічних додатків, для використання рекомендуються три типи ГПВБ: на основі геш-функції, блокового шифру та ЕК [9].

Генератори на базі геш-функції можуть використовувати любу затверджену геш-функцію. ГПВБ на базі геш-функції можна використову-

вати в криптографічних додатках, у яких потрібні різноманітні рівні стійкості захисту, але за умови використання підходящої геш-функції й одержання достатньої ентропії для початкового числа [3, 9].

ГПВБ, які базуються на алгоритмі блокового шифрування, являються універсальними і можуть використовувати любий затверджений алгоритм блокового шифрування. Такі генератори рекомендується переважно використовувати в криптографічних додатках, у яких потрібні різні по стійкості рівні захисту, які визначаються алгоритмом блокового шифрування та довжиною ключа, що застосовуються, а тому і забезпеченням достатньої ентропії для початкового числа [3,9].

На наш погляд, для криптографічних систем з доказовим рівнем стійкості та криптосистем, які не потребують жорстких часових обмежень, найбільш придатним для застосування є ГПВБ на еліптичній кривій, оскільки він має також доказовий теоретичний рівень стійкості. Тому, важливою є задача перевірки відповідності такого генератора певному рівню стійкості та дослідження його статистичних властивостей при зазначеному рівні стійкості.

Стійкість ГПВБ на ЕК засновано на задачі дискретного логарифму в групі точок еліптичної кривої. Сутність її полягає в тому, що для заданих точок P і Q на еліптичній кривій порядку n необхідно знайти таке число a, щоби $Q = aP$.

Для ініціалізації ГПВБ використовується початкове число *seed* довжиною m бітів. Його отримують засобом виконання скалярного множення в групі точок еліптичних кривих, де крива задана над полем, розмір якого приблизно 2^m. У нашому випадку $m \geq 256$. Початкове число, що використовується для визначення початкового значення S ГПВБ, повинно мати ентропію, яка дорівнює максимум 128 бітам, і необхідну стійкість захисту (тобто, ентропія ≥ max (128, стійкість)).

Для забезпечення необхідної стійкості, в процесі реалізації ГПВБ на ЕК необхідно обрати відповідну еліптичну криву і точки кривої. При використанні необов'язкових додаткових вхідних даних, значення цих даних обираються довільними і за допомогою функції гешування перетворюються в m -бітовий рядок.

Реалізація ГПВБ на ЕК складається з вибору відповідної еліптичної кривої і пари точок з додатку D.1 [9] та отримання початкового числа, що використовується для визначення початкового значення для ГПВБ, яке є одним елементом початкового стану. Стан визначається засобом використання таких елементів та перетворень.

1. Лічильник (*reseed_counter*), який вказує на число блоків випадкових даних, генерованих ГПВБ на ЕК протягом поточної реалізації і починаючи з попередньої переініціалізації.

2. Значення (S), яке визначає поточне положення на E, причому S оновлюється протягом кожного запиту псевдовипадкових бітів.

3. Загальні параметри еліптичної кривої (*curve_type*, m, p, a, b, n), де *curve_type* вказує на тип базового поля (ЕК над полем F_p, бінарним полем F_2^m або крива Кобліца); коефіцієнти a і b, які визначають рівняння кривої, і n – порядок точки G.

4. Дві точки P і Q на кривій; де базова точка G для вибраної кривої використовуватиметься як P.

5. Стійкість захисту *strength* забезпечується реалізацією ГПВБ; крива вибирається з умовою забезпечення мінімум *requested_strength* бітів захисту.

6. Булеве значення *prediction_resistance_flag*, що вказує на необхідність переініціалізації кожного разу, коли викликається ГПВБ на ЕК для випадкового *bitstring*.

7. Використання даних ініціалізації у формі односторонньої функції, яка виконується із вхідним значенням *seed*, а потім порівнюється з новим *seed* у час переініціалізації ГПВБ.

2. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ГПВБ НА ЕК

Для тестування ГПВБ на ЕК використовувалася методика NIST STS [10], яка містить 16 статистичних тестів. Ці тести використовуються для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, що породжуються ГВБ або ГПВБ. По сукупності результатів всіх тестів приймається рішення про те, чи буде задана послідовність нулів і одиниць «випадковою» чи ні.

Згідно стандарту ISO/IEC 18031 для ініціалізації генератора необхідно вказати мінімальний рівень стійкості. У якості такого рівня був вибраний мінімальний, тобто значення, яке менше за 2^{80}. Було використано еліптичну криву, яка задана над скінченим полем характеристики більше трьох. Фактична довжина поля складає 192 біта.

У нашій реалізації вектор ініціалізації будується за допомогою генератора випадкових послідовностей, який засновано на одночасному запуску декількох потоків та випадковому зупиненню їх.

У якості функції гешування, яка обумовлена стандартом, ми використали регіональний стандарт ГОСТ 34.311 [11].

Для оцінки мінімальних можливостей генератора тестування проводилось без реініціалізації початкового вектора на кожній ітерації.

Згідно NIST STS було здійснено тестування псевдовипадкової послідовності, а також проведене порівняння властивостей цієї послідовності із властивостями ПВП генераторів на ЕК, що були запропоновані в [2], а також із властивостями генератора псевдовипадкових бітів BBS (тестова вибірка, рекомендована NIST).

Для здійснення тестування були обрані такі параметри:

1. Довжина послідовності, що тестується $n=10^6$ біт.

2. Кількість послідовностей, що тестується $m=100$. Таким чином, обсяг вибірки, що тестується, склав $N=10^6\times100=10^8$ біт.

3. Рівень значимості $\alpha=0{,}01$.

4. Кількість тестів $q=189$. Таким чином, статистичний портрет генератора містить 18900 значень імовірності *P*.

В ідеальному випадку при m=100 і $\alpha=0{,}01$ може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту повинен становити 99%. Але це занадто жорстке правило. Тому застосовувалось правило на основі довірчого інтервалу для r_j. Нижня границя в цьому випадку складе значення $r_{\min}=0{,}96015$. Із цих позицій проаналізуємо результати тестування ПВП.

У табл. 1 наводяться дані по проходженню ПВП тестів за Правилом 1.

Таблиця 1

Генератор	Кількість тестів, у яких тестування пройшли більше 99% послідовностей	Кількість тестів, у яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
ГПВБ на ЕК (ISO/IEC 18031)	129 (68,25%)	189 (100%)
ГПВБ на ЕК 6.13 [2]	138 (73%)	189 (100%)
ГПВБ на ЕК 6.14 [2]	134 (70,9%)	189 (100%)
ГПВБ на ЕК 6.18 [2]	131 (69,3%)	189 (100%)

У табл. 2 представлені зведені результати по проходженню генераторами тестів за Правилом 2.

Таблиця 2

Генератор	Кількість тестів, у яких значення імовірності $P \le 0{,}01$	Кількість тестів, у яких значення імовірності $P \le 0{,}001$
BBS	0	0
ГПВБ на ЕК (ISO/IEC 18031)	1	0
ГПВБ на ЕК 6.13 [2]	2	0
ГПВБ на ЕК 6.14 [2]	3	0
ГПВБ на ЕК 6.18 [2]	2	0

На рис. 1, 2, 3 представлені статистичні портрети деяких генераторів ПВП із вказівкою їхніх параметрів і способів формування. Статистичні портрети інших генераторів представлені в [2].

Як бачимо з отриманих результатів, генератори псевдовипадкових бітів на ЕК, що запропоновані в [2] та в міжнародному стандарті ISO/IEC 18031, показали приблизно ті ж самі результати, які не гірші, ніж результати класичного генератора BBS. А ГПВБ на ЕК 6.13 [2] за правилом 1 показав навіть кращі результати, ніж BBS. Це є доказом надійності схем генерації, що були запропоновані в [2] і в міжнародному стандарті ISO/IEC 18031. Можна зробити висновок, що генератор на ЕК [2] відповідає вимогам міжнародного стандарту ISO/IEC 18031.

Також, за результатами випробувань, можна відмітити, що використання національної функції гешування у поєднанні зі стандартом ISO/IEC 18031 пройшло тестування позитивно та задовольнило вимогам методики NIST STS.

ВИСНОВКИ

У статті [2] та у міжнародному стандарті ISO/IEC 18031 [9] запропоновано подвійний генератор псевдовипадкових послідовностей на еліптичній кривій. Він базується на використанні функції гешування, а також подвійному виконанні скалярного множення точок еліптичної кривої. Стійкість цих генераторів заснована на задачі дискретного логарифму в групі точок еліптичної кривої.

На відміну від ГПВБ на ЕК, який подано у статті [2], ГПВБ стандарту використовує, за необхідністю, повторну ініціалізацію на кожному кроці ітерації, що дозволяє отримати більш якісний статистичний портрет. Але слід зазначити, що повторна ініціалізація уповільнює швидкість отримання випадкової послідовності. Друга відмінність між цими генераторами міститься в можливостях програмної реалізації. При програмній реалізації ГПВБ стандарту є можливість задавати рівень безпечності безпосередньо у програмній реалізації. Таким чином, не має необхідності явно визначати та задавати загальносистемні параметри, що залежать від рівня безпечності, тобто визначати еліптичну криву та базову точку.

На наш погляд, увага до генераторів псевдовипадкових послідовностей на ЕК з боку криптологів зростає. Це обумовлено тим, що такі генератори мають доказовий рівень стійкості. Зважаючи на це, тестування проводилось з мінімальним рівнем стійкості та строгими вимогами щодо вхідних параметрів. Особлива увага приділялась, щоби генератор псевдовипадкових послідовностей задовольнив висунутим вимогам при мінімальному рівні стійкості та мав якісні статистичні характеристики.

Міжнародний стандарт ISO/IEC 18031 «Інформаційні технології – Методи захисту – Генерація випадкових бітів» на сьогодні знаходиться в процесі гармонізації в Україні. За результатами проведеного аналізу щодо вимог до генераторів псевдовипадкових бітів та досліджень генератора псевдовипадкових бітів на ЕК стандарту ISO/IEC 18031 можна зробити висновок про доцільність гармонізації цього стандарту в Україні. Запропоновані в стандарті рішення можуть використовуватись в криптографічних системах захисту

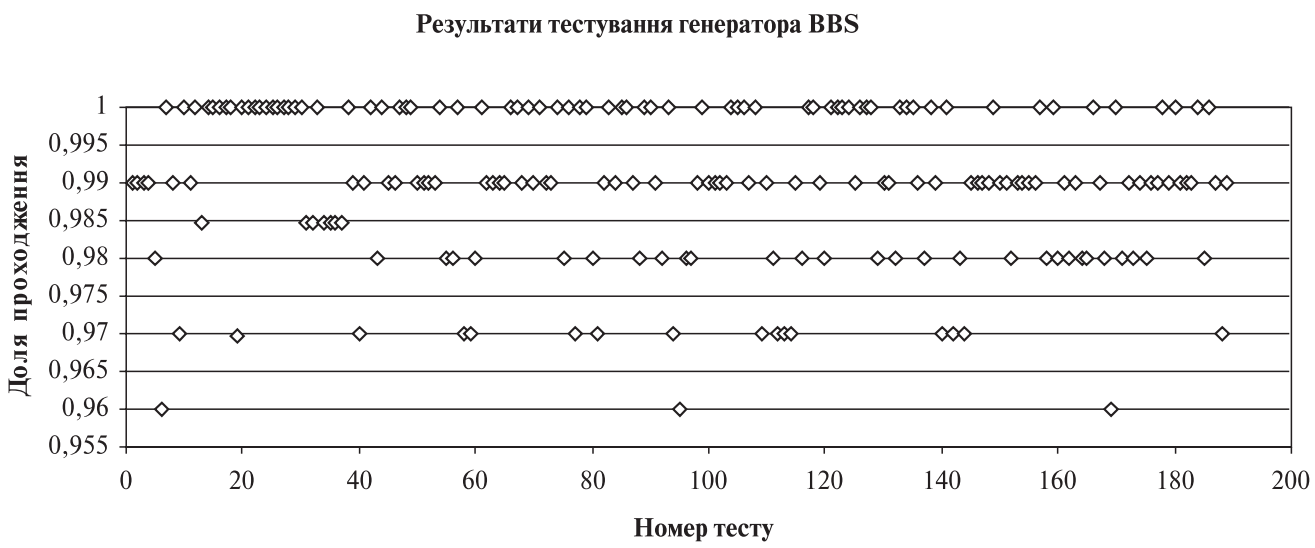

Рис. 1. Результати тестування генератора BBS

Рис. 2. Результати тестування генератора псевдовипадкових бітів
на ЕК міжнародного стандарту ISO/IEC 18031

Рис. 3. Результати тестування генератора псевдовипадкових бітів на ЕК [2]

інформації. Даний міжнародний стандарт може бути взятий за основу при розробці національного стандарту.

Література.

1. *Т.А. Гриненко, Ю.И. Горбенко, С.Ю. Орлова.* Метод формирования и свойства псевдослучайных последовательностей на эллиптических кривых // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С. 119-123.
2. *Т.А. Гриненко, С.И. Збитнев, Д.В. Мялковский.* Методы формирования псевдослучайных последовательностей в группах точек эллиптических кривых. Радиотехника: Всеукр. межвед. науч.-техн. сб. 2002. Вып. 126. С. 115-122.
3. *Т.О. Гріненко, Н.В. Шапочка.* Аналіз детермінованих генераторів псевдовипадкових бітів. Прикладная радиоэлектроника. Том 6, 2007, №2. с.300-305.
4. *Leonard Adleman.* A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In Proceeding of the 20th Annual Symposium on Foundation of Computer Science, page 55-60, IEEE Computer Society, 1979.
5. *Werner Alexi, Benny Chor, Oded Goldreich, and Claus P.Schnorr.* RSA and Rabin functins: Certain parts are as hard as the whole. To appear, SIAM Journal of Computing.
6. *Бондаренко М.Ф., Горбенко И.Д., Качко Е.Г.* Сущность и результаты исследований свойств перспективных стандартов цифровой подписи X9.62 –1998 и распределения ключей X9.63 – 1999 на эллиптических кривых // Радиотехника. 2000. Вып. 114. С.15-24.
7. *Manuel Blum and Silvio Micali.* How to generate cryptographically strong sequences of psevdo-random bits. SIAM Journal of Computing, 13 (4): 850-864, 1984.
8. *Alfred Menezes, et. al.* Handbook af Applied Cryptography – CRC Press, 1997.
9. ISO/IEC 18031. Information technology — Security techniques — Random bit generation, 2005.
10. *А.Потий, С.Орлова, Т.Гриненко.* Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р. С. 206-214.
11. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования.

Надійшла до редколегії 18.09.2009

Гріненко Тетяна Олексіївна, асистент кафедри БІТ ХНУРЕ. Область наукових інтересів: методи та засоби криптографічного захисту інформації.

Погребняк Костянтин Анатолійович, аспірант кафедри БІТ ХНУРЕ, математик ЗАТ «ІІТ». Область наукових інтересів: застосування алгебраїчної геометрії у системах криптографічного захисту інформації, асиметрична криптографія.